October 18, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications commission
445 12 Street, SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

The Internet Commerce Coalition (ICC) files this Ex Parte letter in the above proceeding in order to report a meeting between Jim Halpert and Sydney White of DLA Piper LLP (US) on behalf of the Internet Commerce Coalition with Gigi Sohn, Counselor to Chairman Wheeler, Matt DelNero Bureau Chief Wireline Competition Bureau, Lisa Hone, Associate Bureau Chief Wireline Competition Bureau, and Stephanie Weiner, Wireline Advisor Chairman Wheeler on October 14, 2016. We focused on the following points: 1) the categories of sensitive information under the draft final order are inconsistent with the definition established by the FTC and the White House and do not reflect consumer expectations and 2) the consent requirements for sensitive and non-sensitive data should track the conclusions in the FTC's privacy framework.

Addition of Web Browsing and App Usage as Sensitive Information

During the meeting, we discussed the Protecting the Privacy of Customers of Broadband and Other Telecommunications NPRM and Chairman Wheeler's "Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information". Specifically, Chairman Wheeler's Proposal released on October 6 would have the FCC adopt rules that treat contents of communications, web browsing data and app usage history as equally sensitive data for purposes of the FCC's final broadband privacy rules. If the FCC decides to include contents of communications as part of a category of sensitive information, it should not categorically extend the same level of protection to "non-content" web browsing information and app usage history, as these elements do not necessarily merit additional protections.

We discussed that a core feature of the privacy framework of the Obama Administration and the FTC has been technology-neutral requirements that provide strong, consistent privacy

protections for consumers. This approach benefits consumers because it avoids confusing consumers about the extent to which their privacy is protected online through obscure variations in privacy rules based upon the type of business of the entities with which consumers conduct business online. A consistent approach of the sort that the FTC Comments proposed would also avoid a First Amendment challenge based upon the rules providing an inconsistent approach for Internet advertising activities by ISPs.

We discussed that the FTC Comments did not suggest that non-content web browsing or app usage information should be subject to an opt-in consent requirement, and including this requirement in the final order would create a very different rule for ISPs than the regime that applies for the rest of the Internet ecosystem.

The FTC has examined the question of what qualifies as content, and it is well-established that neither URL addresses of Internet sites visited by a consumer, much less app usage data, are necessarily sensitive information that would require an opt-in consent. And the FTC has determined that implied consent or opt-out choice is appropriate for the use of all non-sensitive web browsing history, and this is the approach that applies throughout the Internet ecosystem today.

We discussed that Section 222 of the Communications Act does not reflect a Congressional judgment that all information handled by telecommunications carriers is sensitive. For example, Section 222 has an exception for "subscriber list information" which is not subject to the same protections as CPNI and which carriers are required to make publically available for competitive reasons.

Operationalizing Compliance

Next, in response to questions regarding how an ISP would implement a distinction between sensitive and non-sensitive web browsing and app usage data, we discussed that Internet companies, including ISPs, routinely implement protections so as to not target advertising or market to consumers on the basis of sensitive data categories, unless opt-in consent is obtained. (These sensitive data categories have been defined in FTC guidance as health information, children's information, financial account data and SSNs; these same categories with the addition of the contents of communications should apply in the Commission's final order.) This distinction is a key part of the Digital Advertising Alliance and Network Advertising Initiative self-regulatory frameworks, in which many Internet companies, including ISPs, participate. The participants are subject to enforcement by government regulators and industry self-regulatory bodies, and the FCC would have even stronger enforcement levers than the FTC has to ensure compliance.

Operationalizing a Sensitivity Based Approach to First Party Marketing

With respect to web browsing history, ISPs operationalize the sensitivity-based approach today using processes similar to those used by many other types of online companies, and it would not be difficult for the FCC to ascertain that such processes comply with the sensitivity-

based approach. For example, many ISPs and other Internet companies operationalize these protections to avoid the use of sensitive information by categorizing website URLs and app usage based on standard industry interest categories established by the Interactive Advertising Bureau ("IAB") and other leading industry associations. This process involves correlating web address or app information (e.g., visit to a barbecue and grilling website) with pre-established "white lists" of permissible interest categories (e.g. food & drink) available from the IAB and other third parties. ISPs and Internet companies operationalize these guidelines via a combination of such "white lists" and "black lists" that isolate and exclude data categorized as sensitive by the FTC.

A white list works by proactively identifying those sites that would be of interest in a particular ad campaign. For example, if a car company wants to target ads for its latest truck to camping enthusiasts, the white list for that ad campaign may include sites that are popular with camping enthusiasts, such as the National Park Service website. ISPs use the advertising industry contextual taxonomy to identify sites that meet these criteria, so that when the ad network notices that an individual has visited white-listed site, that individual may receive ads for the truck.

Companies may also use black lists to prevent the collection or use of potentially sensitive information. In other words, companies proactively identify criteria – consistent with the FTC's definition of sensitive information -- that are impermissible for use in targeting ads. Using a black list, companies that engage in Internet advertising can wall off web browsing and other data from sites that fall into sensitive categories, and therefore avoid using these specific types of content as inputs for advertising programs without user consent. Companies in the Internet advertising ecosystem routinely manage these lists as a way to avoid using web browsing history or other data in a way that raises sensitivity concerns.

Companies also have their own internal compliance measures, such as "data governance" policies that provide oversight and guidance related to what data can be used and under what circumstances, as well as a review and approval process for data use requests that are not currently covered by the policy.

In short, it is simply incorrect to assume that ISPs must intrusively scan the content of customers' web browsing to avoid using sensitive data for advertising and marketing purposes. In fact, it is relatively straightforward for ISPs to categorically exclude, for example, health or other sensitive information for advertising via coding instructions that allow ads to be served based only upon data from white listed sources and/or through algorithms and other coding techniques that exclude data associated with sensitive categories of information.

For this reason, there is no operational compliance barrier that justifies departing from the FTC's recommended approach: to limit the scope of the opt-in requirement to the specific sensitive information categories discussed above. This would apply to a subset of web browsing and app usage information that is actually sensitive, and could be adjusted in the future should the FTC decide that a broader range of categories should be considered sensitive. However, the FCC should reject proposals to categorize all web browsing and app usage as sensitive

information, as they are clearly not treated as such under the FTC and ECPA privacy frameworks.

Notice and Choice

Finally, we discussed a potential alternative to a *sui generis*, special ISP opt-in requirement for web browsing and app usage data. Instead, consistent with Internet advertising self-regulatory frameworks that major ISPs all follow today, the Notice provisions in the final order should require clear notice of use of web browsing and app usage data for marketing and advertising, and customers should have an easy to use method of opting out of these uses. Furthermore, to the extent that an ISP is following one or more self-regulatory frameworks, the fact that a company participates in these self-regulatory frameworks could be noted in the ISPs' privacy notices, providing further self-regulatory program accountability in relation to those commitments.

Conclusion

The final FCC rules should reserve opt-in consent for the elements of sensitive data identified by FTC precedent and the FTC Comments and should otherwise apply the opt-out or implied consent approach set forth in the FTC's 2012 Privacy Report. For example, first-party marketing of an ISP's other products and services should be permissible based on implied consent, as both the FTC and Administration have previously concluded.

Respectfully submitted,

/s/ **Sydney M. White**

Jim Halpert
Sydney M. White
Counsel to Internet Commerce Coalition